

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Civil No. 1:25-cv-00735

vs.

115,773.754567 Tether Tokens (USDT),[¶]

\$2,906 in U.S. Currency, and

One Rose Gold Plated Rolex DateJust Watch,
Model 1603, Serial number 2460257,

Defendants.

/

VERIFIED COMPLAINT FOR FORFEITURE IN REM

NOW COMES Plaintiff, United States of America, by and through its attorneys, Alexis M. Sanford, Acting United States Attorney for the Western District of Michigan, and Joel S. Fauson, Assistant United States Attorney, and states upon information and belief that:

NATURE OF THE ACTION

1. This is a civil forfeiture action filed pursuant to 18 U.S.C. §§ 981(a)(1)(C) and Supplemental Rule G(2) of the Federal Rules of Civil Procedure to forfeit and condemn to the use and benefit of the United States of America 115,773.754567 Tether (USDT) tokens (the Subject Cryptocurrency), \$2,906 seized from 3553 Toronto Trail, Wayland, Michigan on January 30, 2025 (the Subject Cash) and one rose gold plated Rolex DateJust watch, model 1603, serial number 2460257

seized from 3553 Toronto Trial, Wayland, Michigan on January 30, 2025 (the Subject Watch) (altogether, the “Defendant Property”).

THE DEFENDANT IN REM

2. The Defendant Property consists of the Subject Cryptocurrency, the Subject Cash, and the Subject Watch, all of which were seized by the Federal Bureau of Investigation (FBI). The Defendant Property is currently in the custody of the FBI Detroit Field Division, Grand Rapids Resident Agency.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this proceeding pursuant to 28 U.S.C. §§ 1345 and 1355(b)(1)(A), because this action is being commenced by the United States of America as Plaintiff, and the acts giving rise to the basis for forfeiture occurred in this judicial district.

4. Venue is proper before this Court pursuant to 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to forfeiture occurred in this judicial district, and/or pursuant to 28 U.S.C. § 1395(b), because the Subject Cash and Subject watch were found within this judicial district, and/or pursuant to 28 U.S.C. § 1395(c) because the Subject Cryptocurrency was brought into this district.

BASIS FOR FORFEITURE

5. As set forth below, the Defendant Property is subject to forfeiture to the United States pursuant to: 1) 18 U.S.C. § 981(a)(1)(C) because it constitutes any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud, in

violation of 18 U.S.C. § 1349; 2) 18 U.S.C. § 982(a)(2) because it constitutes any property constituting, or derived from, proceeds obtained directly or indirectly traceable to bank fraud, in violation of 18 U.S.C. § 1344 and conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349; and 3) 18 U.S.C. § 982(a)(1) because it constitutes property, real or personal involved in money laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).

BACKGROUND ON CRYPTOCURRENCY

6. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin is the most well-known virtual currency in use.

7. Virtual currency addresses are the specific virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. Each virtual currency address is controlled through a unique corresponding private key—the equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

8. Many virtual currencies publicly record their transactions on what is referred to as the “blockchain.” The blockchain is essentially a distributed public

ledger, run by a decentralized network, containing an immutable record of every transaction that has ever occurred using that blockchain's specific technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

9. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same user. A user of virtual currency can operate multiple addresses at any given time and there is no limit to the number of addresses any user can have.

10. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a single wallet.

BACKGROUND ON TETHER LIMITED

11. Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. The value of USDT is tied to the value of the U.S. dollar. According to Tether Limited, one USDT token is backed by one U.S. dollar held in Tether Limited's reserves. For this reason, USDT is known as a "stablecoin"—a term used to describe a virtual currency that has a value pegged to a fiat currency or the value of a commodity. USDT is hosted on the Ethereum (ETH)

and Tron blockchains, among others.

FACTS SUPPORTING FORFEITURE

Overview of Fraud Scheme Targeting Honor Credit Union Members

12. Honor Credit Union (“Honor”) is headquartered in Berrien Springs, Michigan. Honor is insured by the National Credit Union Administration through the National Credit Union Share Insurance Fund.

13. In or about June 2024, Honor reported to the FBI that some of its members – people who have accounts with Honor – began falling victim to a coordinated campaign of fraudulent SMS-phishing messages.

14. SMS stands for “short message service.” SMS is a text messaging component that allows for text messages to be sent between mobile and internet devices.

15. Phishing is a type of computer, phone, or internet-based scam that utilizes social engineering to deceive a victim into giving up personal information. This personal information generally consists of, but is not limited to, a website user’s username and password and the answers to any security questions. It may also include an individual’s personal identification number (PIN).

16. The scammers’ purpose of the fraudulent SMS-phishing campaign targeting Honor and its members was to obtain access to a member’s account so the scammers could transfer money out of the member’s account for the scammers’ own use and enrichment.

17. The fraudulent SMS-phishing campaign included the following steps:

- a. An Honor member would receive a text message that indicated there was fraud or anomalous activity on their Honor account, and that they needed to click a link in the text message.
- b. If the Honor member clicked the link, it would take them to a fraudulent website that looked similar to Honor's actual website, which would prompt the member to enter their Honor username and password.
- c. If the Honor member did so, they would be prompted to answer three security questions about themselves.
- d. None of the information the member entered would be received by Honor. Instead, the fraudulent website would deliver everything the member had just entered – their username, password, and security answers – to the scammers running the operation.
- e. The scammers would then use the member's information to log into Honor's website and change the member's password, effectively locking them out of their own account. The scammers would then conduct member to member transactions, by sending funds from the victim's Honor account to an Honor account controlled by an accomplice to the scammers.
- f. The accomplice would then withdraw the stolen money from the receiving Honor account, usually by making an electronic payment to an Apple Pay or Cash App account, but sometimes by making an ATM withdrawal.

West Michigan Individuals Help Perpetrate the Fraud Scheme

18. Law enforcement interviewed an Honor member whose bank account had received a fraudulent member-to-member transaction described above. The Honor member said he was recruited by a man named Dixon to provide his debit card, PIN, and online banking credentials for his Honor account. The Honor member responded to a social media post by Dixon seeking people with Honor accounts. The Honor member said they agreed that the member's account would receive money, the member and Dixon would each receive a percentage of the money transferred into the member's account, and then the money would be dispersed.

19. Law enforcement have identified Dixon as Reynardo Dixon. Reynardo Dixon is a resident of Kalamazoo, Michigan. In March 2024, police interviewed Dixon, who said he was a "middleman" who used social media posts to recruit people with accounts capable of receiving online transfers, including people with Honor accounts. When Dixon found willing accomplices and acquired their online banking credentials and debit cards, he would provide the information to Mykalia Brown, a resident of Wayland, Michigan.

20. Dixon began working with Brown after finding her posts on Facebook, through the account "RichLul Whitegurl." Law enforcement has confirmed that RichLul Whitegurl is Mykalia Brown by comparing posted photos to Brown's driver's license photo and references RichLul Whitegurl made on Facebook celebrating her birthday, which is Brown's birthday.

21. Dating back to 2023, Brown used the Facebook profile "RichLul

Whitegurl” to seek access to bank and credit union accounts. Below is a sample of Brown’s Facebook posts:

The image displays six Facebook posts from the page 'RichLul Whitegurl'. The posts are arranged in two columns of three. Each post includes the author's profile picture, name, date, and a snippet of the post content.

- Post 1 (January 29):** Honors ? 20k instant RN RN CALL MY BLUFF. 2 likes, 1 comment. Response: Yes on a Sunday. 18w Like.
- Post 2 (January 20):** Honors credit union ? 20k INSTANT CALL MY MFKIN BLUFF. 1 like.
- Post 3 (December 11, 2023):** Who got Advia credit union ? I got 2k for u rn I just need to transfer my money. 1 like, 2 comments.
- Post 4 (December 29, 2023):** Advia credit Union? We going Instant. 1 like.
- Post 5 (December 2, 2023):** Honor Credit Union & Lake Michigan Credit Union Tap TF IN LETS GO VIRAL ON SATURDAY. 1 like.
- Post 6 (June 16, 2023):** Any active bank accounts hit Me WE STILL GOING UP ON A FRIDAY. 1 like.
- Post 7 (May 24, 2023):** Citi Bank (Chicago) ? HIT ME ASAP FRESH ACCOUNTS ON FIRE. 3 comments.

A sample of Mikayla Brown’s a.k.a. RichLul Whitegurl’s Facebook posts soliciting individuals to access Honor Credit Union and other financial institutions as part of the fraud scheme

22. Brown’s boyfriend is Savon Johnson. Savon Johnson is a resident of Kalamazoo, Michigan.

23. Savon Johnson participated in the fraud scheme, at least in part, by withdrawing victims’ money from accomplice accounts at Honor Credit Union. Below

is a sample of Honor ATM surveillance footage of Johnson withdrawing fraud money:



Honor Credit Union surveillance footage of Savon Johnson withdrawing fraudulently-obtained funds

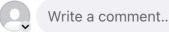
24. Tyvion Anderson is a friend of Savon Johnson. Tyvion Anderson is a resident of Kalamazoo, Michigan. Tyvion Anderson also withdrew victim funds from Honor Credit Union.

25. Tyvion Anderson operates a Facebook account under the username Bobby Boucher (TyKoon). Anderson used the Bobby Boucher account to recruit people to provide bank or credit union account information, including Honor Credit Union account information. Below is a sample of Anderson's Facebook posts:

 **Bobby Boucher**
21 hours ago · 

Who got Lake Michigan credit union

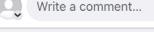
 Like  Comment  Share

 Write a comment... 

 **Bobby Boucher**
2 days ago · 

Any credit union with business account let's make some money

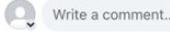
 Like  Comment  Share

 Write a comment... 

 **Bobby Boucher**
4 days ago · 

All major banks I got bag for you
All credit unions I got bag for you
Aged accounts only

 1  Comment  Share

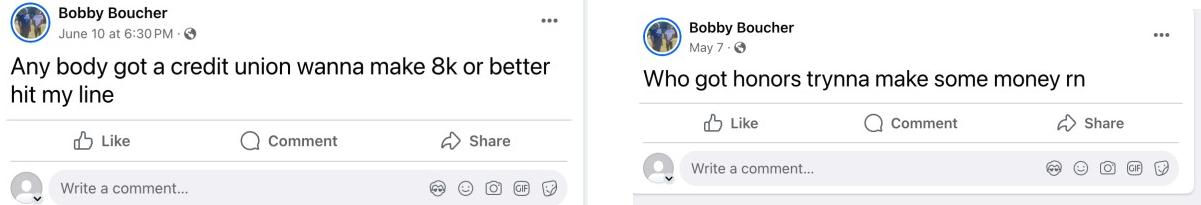
 Write a comment... 

 **Bobby Boucher**
4 days ago · 

Swing me any aged credit union I'm going instant today only

 1  Comment  Share





A sample of Tyvion Anderson's a.k.a. Bobby Boucher's Facebook posts soliciting individuals to access Honor Credit Union and other financial institutions as part of the fraud scheme

26. The scammers have stolen at least \$1.2 million in Honor Credit Union member funds.

Fraud Funds are Dispersed and Converted into Cryptocurrency to Conceal and Disguise the Nature, Location, Source, and Ownership of the Funds

27. The scammers, including Mykalia Brown, Savon Johnson, and Tyvion Anderson transferred fraud funds to electronic payment platforms including, but not limited to, Apple Pay and Cash App.

28. Cash App is a mobile payment service that allows users to send and receive money. It also allows its users to buy and sell the cryptocurrency Bitcoin (“BTC”) directly on their application.

29. Brown, Johnson, and Anderson each have a Cash App account. Each of them received deposits of fraud funds on numerous occasions into their respective Cash App accounts. They then purchased BTC with the incoming deposit money and transferred the BTC to a series of identified BTC addresses.

30. From at least January 1, 2024 until April 30, 2024, the same pattern repeated: an incoming transfer of fraudulently-obtained funds to Cash App, a BTC purchase, and a BTC transfer to a series of identified BTC addresses. This pattern occurred in Johnson’s Cash App account at least 15 times, in Brown’s CashApp

account at least 20 times, and in Anderson’s Cash App account at least 18 times. The cumulative amount of BTC sent from the accounts was approximately 1.165 BTC, or \$78,799 based on the BTC’s market value as of October 24, 2024.

31. The BTC constituting the fraudulently obtained funds from Honor Credit Union members was transferred and co-mingled into a handful of BTC wallets before being deposited into an identified BTC address ending in “55MTKt” (the “BTC Address”) held at the virtual currency exchange MEXC.com. MEXC.com is an online virtual currency exchange headquartered in the Seychelles.

32. Between January 4, 2024 and May 1, 2024, the BTC Address received 21 deposits that totaled approximately 2.37 BTC. During this same timeframe, there were 20 withdrawals from the BTC Address to the USDT address TBsxyoyFRnHvTfX1xGMCKyazJyF35tznAx (the “USDT Address”). Specifically, 19 of the 20 withdrawals from the BTC Address to the USDT Address took place within 25 minutes of the incoming BTC deposit. The 20 withdrawals totaled 122,873 USDT, the equivalent of \$122,873. To transfer Bitcoin into USDT, the operator of the BTC Address, , used a capability called a “swap feature,” which converts one type of cryptocurrency to another.

33. IP addresses associated with the accounts that were involved with moving the fraud funds from Honor Credit Union into the BTC Address and finally into the USDT Address included direct matches. For example, on January 4, 2024, an IP address – 45.118.159.187 – was used to access an Honor account that contained fraud funds two separate times and was also used to conduct a BTC to USDT swap

that sent funds from the BTC Address to the USDT Address. Similarly, on January 5, 2024, an IP address – 202.173.125.117 – was used to access an Honor account containing fraudulently-obtained funds and was also used to conduct a BTC to USDT swap that sent funds from the BTC Address to the USDT Address, which constituted part of the Subject Cryptocurrency.

34. The IP addresses 45.118.159.187 and 202.173.125.117 are associated with an Internet Service Provider headquartered in New Delhi, India.

35. After the Federal Bureau of Investigation seized the Subject Cryptocurrency, the FBI was contacted by a man who identified himself as Sanchit Jain from the country of India. Jain advised he contacted Tether regarding the USDT Address and Tether referred him to the FBI. Jain claimed he was a “bug bounty hunter” from India and was the owner of the USDT Address that contained the Subject Cryptocurrency.

36. Wire fraud, in violation of 18 U.S.C. § 1343 and bank fraud, in violation of 18 U.S.C. § 1344 constitute “specified unlawful activity” as defined at 18 U.S.C. § 1956(c)(7)(A) and 18 U.S.C. § 1961(1)(B).

37. The scammers moved the fraudulently-obtained funds from Honor Credit Union accomplice accounts into Cash App, purchased BTC via Cash App, and then swapped the BTC for USDT to conceal and disguise the nature, the location, and the source of the wire fraud proceeds and the bank fraud proceeds.

Mykalia Brown’s Phone Number and Savon Johnson’s Email Address are Connected to Phone Numbers that Sent Out SMS Phishing Messages

38. On February 2, 2024, phone numbers 616-370-8788 and 616-367-4680

sent out SMS phishing messages to Honor Credit Union members. On March 5, 2024 and March 7, 2024, phone number 616-877-6106 sent out SMS phishing messages to Honor Credit Union members. These messages asked Honor Credit Union members to click on a malicious link.

39. The phone numbers that sent out SMS Phishing messages on February 2, 2024, were assigned by PureTalk, a reseller of AT&T service. The FBI subpoenaed PureTalk and learned that the PureTalk subscriber phone number and email address for phone numbers 616-370-8788 and 616-367-4680 are Mykalia Brown's. Specifically, the subscriber phone number and email address from PureTalk, 708-270-8983 and kailaawhite4@gmail.com, were identified as the user account email and phone number from two phones seized at Brown's home on January 30, 2025.

40. The phone number that sent out SMS phishing messages on March 7, 2024 was issued by AirVoice Wireless, a wireless phone service provider. The FBI subpoenaed AirVoice Wireless and determined that the AirVoice Wireless subscriber email address for 616-877-6106 is Savon Johnson's email address, jt339199@gmail.com.

The Subject Cash and Subject Watch are Seized from Mykalia Brown's Residence

41. On January 30, 2025, the FBI executed a search warrant at Mykalia Brown's residence, 3553 Toronto Trail, Wayland, Michigan. The FBI seized ten cell phones, the Subject Cash and the Subject Watch.

42. Brown was home while the search warrant was executed. She was informed that she was not being arrested and was free to leave. Brown voluntarily

spoke with investigators. She informed the investigators that she did not work and gets child support, food stamps, and money from her mother and her boyfriend. She also said that the Subject Watch was a gift but did not specify from whom.

CLAIM I

43. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

44. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

CLAIM II

45. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

46. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes any property, real or personal, which constitutes or is derived from proceeds traceable to a conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349.

CLAIM III

47. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

48. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 982(a)(2) because it constitutes any property constituting, or derived from, proceeds obtained directly or indirectly traceable to bank fraud, in violation of 18 U.S.C. § 1344.

CLAIM IV

49. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

50. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 982(a)(2) because it constitutes any property constituting, or derived from, proceeds obtained directly or indirectly traceable to a conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349.

CLAIM V

51. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

52. The Subject Cryptocurrency is forfeitable to the United States pursuant to 18 U.S.C. § 982(a)(1) because it constitutes property, real or personal, involved in money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

CLAIM VI

53. Plaintiff hereby re-alleges paragraphs 1 – 42 as referenced above.

54. The Subject Cryptocurrency is forfeitable to the United States pursuant to 18 U.S.C. § 982(a)(1) because it constitutes property, real or personal, involved in a conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).

REQUESTED RELIEF

Wherefore, the United States requests that the Court issue a warrant for the arrest of the Defendant Property, that due notice be given to all interested parties to appear and show cause why forfeiture to the United States of America should not be decreed; and that the Defendant Property be condemned and forfeited to the United States of America and be delivered into the custody of the Federal Bureau of Investigation for disposition according to law; and for such other relief as this Court may deem just and proper.

ALEXIS M. SANFORD
Acting United States Attorney



Dated: July 1, 2025

JOEL S. FAUSON
Assistant United States Attorney
P.O. Box 208
Grand Rapids, MI 49501-0208
(616) 456-2404

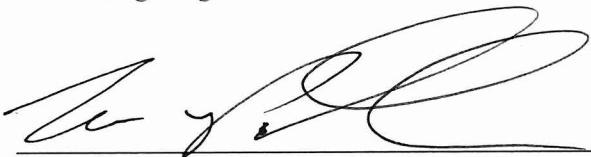
VERIFICATION

I am a Special Agent with the Federal Bureau of Investigation with personal involvement in this investigation.

I have read the contents of the foregoing Verified Complaint for Forfeiture In Rem, and the statements contained therein are true to the best of my knowledge and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: 7/1/2025



TOM PELLER
Special Agent
Federal Bureau of Investigation